(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－336169

(43)公開日　平成10年(1998)12月18日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ
			６７５Ｄ

審査請求　有　　請求項の数23　ＯＬ　（全 25 頁）

(21)出願番号　特願平9－138724

(22)出願日　平成９年(1997)５月28日

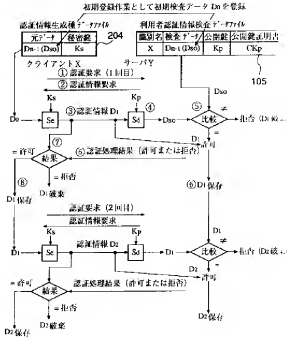
(71)出願人　591030237
日本ユニシス株式会社
東京都港区赤坂２丁目17番51号
(72)発明者　八津川　直伸
東京都港区赤坂２－17－51　日本ユニシス株式会社内
(74)代理人　弁理士　大塚　康徳　（外１名）

(54)【発明の名称】　認証方法、認証装置、記憶媒体、認証サーバ及び認証端末装置

(57)【要約】　（修正有）

【課題】　盗まれた認証情報の第三者による再利用が困難な認証方法を提案する。

【解決手段】　前もってサーバにクライアントの認証情報を検査するための第１の検査データ（値＝D_{n-1}）を保存しておき、クライアントも、認証情報を生成するための第１の種データ（値＝D_{n-1}）を保存しておく。クライアントは、サーバから送られてきた認証情報要求に対して、クライアントの秘密鍵（K_S）を用いて暗号化して認証情報（値＝D_n）を生成し、サーバに送ることによって答える。サーバは、クライアントの公開鍵（K_p）によって復号化して第２の検査データ（値＝D_{n-1}）を生成し、第１の検査データ（値＝D_{n-1}）と比較し、一致した場合には、認証要求を許可するとともに、第１の検査データに換えて認証情報（D_n）を保存する。クライアントは、許可を受けると、第１の種データ（値＝D_{n-1}）に換えて、認証情報（値＝D_n）を第２の種データとして保存する。



【特許請求の範囲】
【請求項１】　認証要求者からの認証の要求に対して、公開鍵暗号方式により認証者が認証要求者を認証する方法であって、
前もって認証者は、認証要求者の認証情報を検査するための第１の検査情報を保存しておく保存工程と、
前記認証要求者は前記認証者に認証要求を送る認証要求送出工程と、
前記認証者は、前記認証要求者から送られてきた認証要求に対して、認証情報要求を前記認証者に送ることによって応る認証情報要求工程と、
前記認証要求者は、前記認証情報要求に応答して、認証情報を生成するために前記認証要求者が自身が保持している第１の種情報を前記認証要求者の秘密鍵を用いて暗号化して生成した第１の認証情報を前記認証者に送るとともに、生成した前記第１の認証情報を次回の認証要求のための第２の種情報として前記保持していた第１の種情報に換えて保存する認証情報送出工程と、
前記認証者は、前記認証要求者から送られてきた前記第１の認証情報を前記認証要求者の公開鍵によって復号化することにより、第２の検査情報を生成し、この第２の検査情報を前記前もって保存していた前記第１の検査情報と比較する比較工程と、
前記認証者は、前記第２の検査情報が前記第１の検査情報と一致した場合には、前記認証要求を許可する旨を前記認証要求者に通知すると共に、前記第１の検査情報に代えて前記第２の検査情報を保存する更新工程とを具備することを特徴とする認証方法。
【請求項２】　複数の認証要求者からの認証要求に対して認証を与えるための認証情報を保存する認証サーバであって、
認証要求者毎に認証要求者の認証情報を検査するための検査情報を記憶する手段と、
任意の認証要求者からの認証要求を受けると、認証情報要求メッセージをその認証者に送る手段と、
その認証要求者から送られてきた認証情報を、その認証要求者の公開鍵によって復号化して、新たに検査情報を生成し、この新たに生成した検査情報を前記前もって保存していた検査情報と比較する手段と、
前記新たに生成した検査情報が前記保存していた検査情報と一致した場合に、前記認証要求を許可すると共に、前記保存していた検査情報に代えて前記新たに生成した検査情報を保存する手段と、を具備する認証サーバ。
【請求項３】　外部の認証サーバの支援により、認証要求者からの認証要求に対する認証を与える認証装置であって、
前記認証要求者を認証する認証情報を生成するための種情報を記憶する記憶手段と、
前記認証サーバに認証要求メッセージを送ると共に、この認証要求メッセージに応答する前記認証サーバからの認証情報要求メッセージを受ける送受信手段と、
前記認証サーバからの認証情報要求メッセージに対して、前記記憶手段に記憶している前記種情報を秘密鍵を用いて暗号化することにより認証情報を生成する暗号化手段と、
生成した認証情報を前記認証サーバに送ると共に、前記記憶手段において、記憶されている前記種情報に換えてこの生成された認証情報を記憶する認証送出手段とを具備する認証装置。
【請求項４】　外部の認証サーバの支援により、認証要求者からの記憶媒体を介した認証要求に対して認証を与える認証端末装置であって、
本体と、
認証要求者を認証する認証情報を生成するための種情報とその認証要求者についての秘密鍵と前記種情報から前記秘密鍵を用いて認証情報を生成するプログラムとを記憶する記憶媒体を受け容れるためのインタフェース手段とを有し、
前記本体は、
前記認証要求者からの認証要求を受ける受信手段と、
この認証要求に応答して前記認証サーバに認証要求メッセージを送ると共に、この認証要求に応答する前記認証サーバからの認証情報要求メッセージを受ける要求手段と、
認証情報要求メッセージに応答して、前記インタフェース手段を介して、前記記憶媒体中のプログラムを実行させる指令手段であって、前記プログラムに対して、前記種情報から前記秘密鍵を用いてこの認証要求者の認証情報を生成せしめ、生成した認証情報を前記インタフェース手段を介して前記本体に送り返せしめると共に、この生成した認証情報により前記記憶媒体中の前記種情報を更新せしめる指令手段と、
送り返された認証情報を前記認証サーバに送る認証情報送出手段とを具備する認証端末装置。
【請求項５】　外部の認証サーバの支援により、認証要求者からの認証要求に対する認証を与える認証プログラムを記憶する記憶媒体であって、
前記認証プログラムは、
前記認証要求者を認証する認証情報を生成するための種情報を所定の記憶手段に記憶させる第１のプログラムコードと、
前記認証サーバに認証要求メッセージを送る第２のプログラムコードと、
前記認証サーバからの認証要求メッセージを受け取る第３のプログラムコードと、
認証情報要求メッセージに対して、前記記憶手段に記憶している前記種情報から秘密鍵を用いて認証情報を生成する第４のプログラムコードと、
生成した認証情報を前記認証サーバに送ると共に、前記古い種情報に換えて、この生成した認証情報を新たな種

情報として記憶する第５のプログラムコードとを具備することを特徴とする記憶媒体。

【請求項６】　前記認証情報送出工程は、
認証要求を許可する旨の通知を受けた場合に、前記第１の種情報を前記第２の種情報で置き換えて保存し、通知を受けなかった場合には、置き換え保存を行わないことを特徴とする請求項１に記載の認証方法。

【請求項７】　前記認証送出手段は、
認証要求を許可する旨の通知を前記認証サーバから受けた場合に、前記種情報の更新を行い、通知を受けなかった場合には、更新を行わないことを特徴とする請求項３に記載の認証装置。

【請求項８】　前記指令手段は、前記記憶媒体中のプログラムに、認証要求を許可する旨の通知を前記認証サーバから受けた場合に、前記種情報の更新を行なわせ、通知を受けなかった場合には、更新を行わせないことを特徴とする請求項４に記載の認証端末装置。

【請求項９】　前記第５のプログラムコードは、前記記憶媒体中のプログラムに、認証要求を許可する旨の通知を前記認証サーバから受けた場合に、前記種情報の更新を行ない、通知を受けなかった場合には、更新を行わない第６のプログラムコードを含むことを特徴とする請求項５に記載の記憶媒体。

【請求項１０】　前記第１の種情報の初期値として前記認証要求者の識別情報を用いることを特徴とする請求項１に記載の認証方法。

【請求項１１】　前記種情報の初期値として前記認証要求者の識別情報を用いることを特徴とする請求項３に記載の認証装置。

【請求項１２】　前記種情報の初期値として前記認証要求者の識別情報を用いることを特徴とする請求項４に記載の認証端末装置。

【請求項１３】　前記認証情報送出工程では、認証情報を公開鍵証明書付きで前記認証者に送ることを特徴とする請求項１に記載の認証方法。

【請求項１４】　前記認証情報送出手段は、認証情報を公開鍵証明書付きで前記認証サーバに送ることを特徴とする請求項３に記載の認証装置。

【請求項１５】　前記認証情報送出手段は、認証情報を公開鍵証明書付きで前記認証サーバに送ることを特徴とする請求項４に記載の認証端末装置。

【請求項１６】　前記記憶手段は、認証要求者毎の公開鍵を検査情報と共に記憶することを特徴とする請求項２に記載の認証サーバ。

【請求項１７】　認証者は、送られてきた公開鍵証明書を保存することを特徴とする請求項１３に記載の認証方法。

【請求項１８】　前記第１の検査情報が前記第２の検査情報と一致しなかった場合には前記認証要求者による前記認証要求を拒否することを特徴とする請求項１に記載の認証方法。

【請求項１９】　前記新たに生成した検査情報が前記保存していた検査情報と一致しなかった場合には前記認証要求者による前記認証要求を拒否することを特徴とする請求項２に記載の認証サーバ。

【請求項２０】　前記認証要求者の秘密鍵は、真正の持ち主のみが復号化できるように暗号化されていることを特徴とする請求項１に記載の認証方法。

【請求項２１】　前記記憶媒体はＩＣカードであることを特徴とする請求項４に記載の認証端末装置。

【請求項２２】　前記記憶媒体はパスワードを更に記憶し、更に、前記認証要求者から入力されたパスワードと前記記憶媒体に記憶されたパスワードとを比較し、一致したときにのみ、前記記憶媒体は認証情報を前記本体に送り返すことを特徴とする請求項４に記載の認証端末装置。

【請求項２３】　秘密鍵を用いた種情報から認証情報への変換は記憶媒体においてのみ行われ、前記秘密鍵は前記本体側に送られないようにされたことを特徴とする請求項４に記載の認証端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えばネットワークを介した相手方の認証方法、認証装置、認証装置のためのプログラムを記憶した記憶媒体、その認証に関与する認証者としての認証サーバに関する。

【０００２】

【従来の技術】情報処理システムが社会活動のあらゆる局面において中心的な役割を演じるようになった現在、ネットワークを介した個人間や個人―企業間或いは企業間の情報通信に対するセキュリティ保護が緊急の課題となっている。特に昨今のネットワーク・システムのオープン化・汎用化により、機密情報転送や電子商取引(Electronic Commerce)のような分野に対し、セキュリティ機能は必要不可欠なものとなっている。例えば、企業間、個人間或いはそれら相互間で法律行為をなす場合、従来（現在でも）、物理的な紙を使用して契約書等を作成し、署名し、印鑑を押印し、更に必要に応じ、印鑑登録証や公証人による公正証書を添付し、次にこれら文書を相手方に送付する際、書留にし、或いは内容証明郵便にする。

【０００３】このような物理的な書類を中心にした行為を全て、電子的な情報通信によって安全に代替ならしめるものが、ネットワーク・セキュリティ技術である。コンピュータとネットワークによる情報通信網が全世界規模に達した現在、このような要求は増大の一途である。ネットワーク・セキュリティの目的は、ネットワークの安全保護に有り、ネットワーク・システムの機密度に応じた情報をさまざまな脅威から保護することであるとされている。一般的には、①機密性(Confidentiality)、

②完全性(Integrity)、③可用性(Availability)、④否認拒否(Non-Repudiation)を維持することと定義されている。一方、ネットワークに対して想定される代表的脅威としては、盗聴、漏洩、なりすまし、改ざん／偽造、不正侵入／不正アクセス、横取り、事実の否認、破壊などである。

【０００４】また、ネットワークセキュリティための要素技術として、秘匿・保全技術、認証技術、鍵配送技術、否認拒否技術、第三者信用機関、アクセス管理、セキュリティ監査、セキュリティ評価基準などがある。ネットワーク・システムを介した情報通信を行うとき、そのシステムを誰がどのように利用したかということを確認したり、制御、管理することはセキュリティを維持する上において重要であり且つ必須である。システム内で起こる大方のイベントは、情報通信に関わる特定の実体（エンティティ）に起因しているはずであり、従ってそれらの認識はセキュリティ確保の基本であると言える。

【０００５】認証とは、情報通信に関与した実体（エンティティ：人間、人間の代理として機能するプロセス、ソフトウエア、ハードウエア、通信データ等）が正当なものであるか否かを確認することであると考えられる。一般的には、認証する実体別に第１図のように分類することができる。エンティティ認証は情報通信に関わる実体、例えばメッセージの送受信等の正当性を確認することであり、一方、メッセージ認証は、それら送受信メッセージの正当性を確認することであると言える。尚、エンティティ認証は利用者認証と呼ばれることもある。

【０００６】エンティティ認証機構は、エンティティ識別処理とエンティティ認証処理に分けられる。前者は、システムの利用者が誰であるかを識別するもので、後者はその利用者が正当な本人であるか否かを確認する処理である。前者には、一般的に利用者識別名(User-id)等が用いられるが、これは公知の識別子であり、本人だけが持ち合わせる情報（パスワードや暗証番号等）を用いた本来の認証処理は、後者の処理に委ねられる。

【０００７】以下のエンティティ認証機構は、このエンティティ認証処理について記述している。エンティティ認証機構には、認証に用いる情報のあり方により、大きく、知識利用、暗号利用、所有物利用、生体特徴利用の４つに分類できる。これらを順に説明する。

【０００８】（知識利用）知識利用によるエンティティ認証とは、エンティティを認証するために必要な情報を予め登録しておき、認証されるべきエンティティがその情報を知っているか否かでそのエンティティの正当性を確認する方法である。個人認証等で最も良く用いられているのが「パスワード」や「暗証番号」或いは「その個人にしか知り得ない情報（住所、生年月日等）」である。

【０００９】大抵のシステムでは、「パスワード」により利用者認証を行っている。このような知識利用によるエンティティ認証は導入が比較的簡単で有効であるが、覚え易い文字列を使用したり、人目に付き易いところにメモしがちで容易に他人に見破られたり、通信中に盗聴されたりする危険性が高い。また、パスワード送信時に暗号化しても毎回同じパスワードであればそれをそのまま盗用し、再利用することで（リプレイ攻撃）で「なりすまし」が可能である。さらに、サーバ側のパスワード・ファイル（通常利用者のパスワードをキーとして暗号化された保存されている）が辞書攻撃によって破られる可能性もある。

【００１０】これらの脅威に対抗するためには、毎回パスワードを変更する等の工夫が必要となる。そのため知識利用のエンティティ認証においては、例えば、ワンタイム・パスワード方式やチャレンジ・レスポンス方式等のような一方向性関数や乱数を利用した、高度な一回限りのパスワード方式が考案されている。以下に各々の方式について述べる。

（１）ワンタイム・パスワード方式

文字通り一回限りのパスワード認証方式で、Bellcore (o.U.S.Aによって提唱され、インターネット標準としてもＲＦＣ化されている(RFC-1938)。以下に、最も有名なＳ／Ｋｅｙ方式の処理概要を説明する。

【００１１】Ｓ／Ｋｅｙ方式は、Ａをクライアント、Ｂを認証サーバとすると、

１：　一方向性乱数ｆを準備する。

２：　Ａは秘密の乱数Ｒと公開の種と呼ばれる任意の数値Ｓを生成する。

３：　Ｑ＝Ｒ＋Ｓとし、ｆ(Ｑ)，ｆ(ｆ(Ｑ))，ｆ(ｆ(ｆ(Ｑ)))，…を計算し、それらをX_1，X_2，X_3，…，X_{100}，X_{101}とする。

【００１２】４：　ＡはX_1，…，X_{100}およびＲを秘密に保持し、ＢにはX_{101}を何らかの方法（オフライン）で渡し、Ｂはそれらを保持する。

５：　Ａが初めてログインする際、パスワードとしてX_{100}をＢに送信する。

６：　Ｂは（X_{100}）を計算し、保持していたX_{101}と比べる。もし、一致すればログインを許可し、一致しなければログインを拒否する。ログインが許可された場合、ＢはX_{101}を捨て、X_{100}を保持する。

【００１３】７：　Ａが次にログインするときは、次のパスワードX_{99}を使用する。Ｂ側の以降の処理は同様に行われる。

Ｓ／Ｋｅｙ方式の長所として、

・一回限りのパスワードなので、通信途上で第三者が盗聴しても再利用が不可能である。

【００１４】・サーバＢのファイル上に保持しているパスワードは、次回ログイン時のパスワードを検査するためのものであり、これが盗まれても支障はない。

・関数ｆは一方向性関数なので、X_nが盗聴されてもX_{n-1}が計算できない。従って、ｆが第三者に知られても

支障ない。
しかし、Ｓ／Ｋｅｙ方式の短所として、
・上の場合で、１００個パスワードを使い切ると、サーバの認証プログラムを再初期化する手間が必要である。
【００１５】・実際のシステムでは上記再初期化をオンラインで可能ならに、サーバ側では常に乱数Ｒを保持する必要がある。即ち、再初期化時、クライアントは以前とは異なった種Ｓ′のみをサーバにオンラインで送信し（Ｓ′は盗聴されても問題ない）、サーバは保持していたＲを用いて新たにＱ′＝Ｒ＋Ｓ′を計算し、これから新たなＸ′101を生成する。このため、第三者がなんらかの方法でサーバに侵入したり、或いはサーバ管理者が悪意でこの乱数を得ると、パスワードが生成できクライアントＡになりすますことが出来る。
（２）チャレンジ・レスポンス方式
これは、パスワード認証における盗聴対策の一種で、代表的なものに、ＣＨＡＰ(Challenge Authentication Protocol，RFC-1334)方式がある。このＣＨＡＰ方式において、認証要求者Ａが認証者Ｂに認証してもらう手順は第２図の通りである。
【００１６】チャレンジ・レスポンス方式は、チャレンジが毎回変化するので、第三者が図中②のメッセージを盗聴していも再利用が不可能であるとの長所がある反面、Ｂ上にＡのパスワードが保持されているので、Ｂの管理者自身がそれを悪用し、クライアントＡになりすまして不正を行うことができるという短所を指摘されている。
【００１７】〈暗号利用〉エンティティ認証に暗号を利用するとは、暗号技術を用いて当事者以外には偽造が困難な認証情報を生成し、それを当事者同士が交換・検査することにより当事者（エンティティ）の正当性を確認する技法である。
（１）デジタル署名
デジタル署名は、従来の書面取り引きにおける署名や印鑑による本人確認を電子媒体上で行う機構で、機能的には次の３条件を満たすことが要件であると考えられている。
【００１８】
①署名文が第三者によって偽造できない。
②署名文が受信者によって偽造できない。
③署名文の内容およびそれを送った事実を送信者が後で否定できない。
現状では、②および③の要件を満たすために公開鍵暗号方式の利用が必須である。公開暗号方式は、１９７６年にスタンフォード大学のディフィ(Diffie)とヘルマン(Hellman)によって発表された概念で、一対の暗号化鍵と復号化鍵とが異なり、復号化鍵のみを秘密に保持し、暗号化鍵は公開して構わない。そのために、鍵の配送が容易であること、秘密に保持する鍵の種類が少なくて済むこと、認証機能（デジタル署名）を有すること、等の特徴を有するといわれている。公開鍵暗号方式の一般モデルを第３図に示す。
【００１９】この公開鍵と秘密鍵の関係を逆にするとデジタル署名機能となる。即ち、送信者のみが知る秘密鍵で平文を暗号化し受信者に送信する。また、受信者は、送信者の公開鍵で復号化し平文を得る。この場合、暗号化鍵は送信者しか知らないので、暗号文が第三者および受信者によって偽造できないことになる。また、暗号化鍵を持つ本人にしか平文の内容を暗号化し送信することができないため、後になって暗号文の内容およびそれを送った事実を送信者が否定できず、上述のデジタル署名の要件を満たす。
【００２０】現在、この公開鍵暗号の概念を実現した世界で最も有力なアルゴリズムとして、ＭＩＴのRivest、ShamirおよびAdlemanによって開発され、それぞれの頭文字を採って命名されたＲＳＡ暗号がある。尚、国際的に標準化されつつあるデジタル署名方式としては、次の２つがある。
・認証子照合法(with appendix)－－ISO/IEC CD 14888 PART1/2/3(Sep 21, 1995)
・通信文復元法(giving message recovery)－－ISO/IEC 9796:1991(E)
実際に広く利用されているのは前者の認証子照合法であり、その概要を第４図に示す。
【００２１】デジタル署名を用いて受信者が送信者の正当性を検証するためには、送信者の公開鍵が真の差出人のものである保証が必要である。例えば、物理的印鑑が正当なものであることを証明する印鑑登録証に相当するものがデジタル署名に必要となる。この保証のために信頼出来る第三者による公開鍵証明書制度が設けられ、その発行機関はＣＡ(Certification Authority)と呼ばれる。ＣＡはインターネット標準(RFC1421-1424)として制定され、公開鍵証明書の発行と管理を行う。
【００２２】証明書のフォーマットは、国際標準（Ｘ．５０９→ＩＳＯ９５９４－８）として制定されており、既に、Ｘ．５０９は第三版が出ており、今後それに対応したＩＳＯ標準も制定される予定である。証明書は、利用者の識別子、利用者の公開鍵、証明書の有効期限、シリアル番号、発行機関名、発行機関のディジタル署名等の項目からなり、これらの後に当該ＣＡの電子署名が付される。
【００２３】第４図の例において、送信者Ａは送信本文およびそれに施したＡのデジタル署名と共に、このＡの公開鍵証明書をＢに送信する。受信者Ｂはまずこの公開鍵証明書のＣＡによるデジタル署名を検査することにより、Ａの公開鍵証明書の正当性を確認する。これが正当であればＢは正当なＡの公開鍵を入手できたことになる。この後、ＢはＡのデジタル署名を検査することにより送信者認証を行う。
【００２４】認証子照合法の長所として、厳格なＣＡが

存在し、且つ送信者が自身の秘密鍵を厳密に保持できれば、第三者による「なりすまし」は一般的に困難であるとの点が指摘されている。しかしながら、ネットワークを介したリモートログインにおいて、署名をリモートログインのためのパスワードとして使用した（即ちデジタル署名を相手認証情報として用いる）場合には、第三者がそれを盗聴しそのまま再利用する（リプレイ攻撃）ことで「なりすまし」が可能であるという短所もある。

（２）デジタル署名付認証トークン方式

これは（１）の方式のリプレイ攻撃に対する強度を改善したものと言える。第５図に、デジタル署名付認証トークン方式の処理の概略を示す。

【００２５】即ち本方式の前提として、クライアントＡはＣＡの秘密鍵によってデジタル署名されたＡの公開鍵証明書を、またサーバＢはＣＡの公開鍵を保持しているものとする。この状態においてクライアントＡは認証情報（以下、認証トークンと称する）として、次の①から④から組み立てられたものをサーバＢに転送する。この認証トークンには、トークン作成時のタイムスタンプＴが含まれている。

【００２６】

①：Ａの公開鍵証明書（Ｃａ）

②：タイムスタンプ（Ｔ）

③：受信者ｉｄ：ＢのE-Mailアドレス等

④：②+③のデジタル署名（Ｓａ）

この認証トークンを受信したサーバＢは先ず署名の検査を行い、タイムスタンプＴ等が改ざんされていないことを確認の上、このＴと現在時刻とを比較する。もし比較結果がほぼ等しければクライアントＡのログインを許可する。

【００２７】しかし、Ｔが一定時間以上過去の時刻であれば、この認証トークンがＡおよびＢ以外の第三者によって再利用（リプレイ攻撃）されているものと見做してログインを拒否する。このトークン方式は、厳格なＣＡが存在し、且つ送信者が自身の秘密鍵を厳密に保持できれば、第三者による「なりすまし」はかなり困難であるとの長所がある反面、一定時間内であれば、盗聴した認証トークンをそのまま再利用すること（リプレイ攻撃）で「なりすまし」が可能であるとの短所も有している。

（３）ＳＳＨ(Secure SHell)方式

ＳＳＨ方式はＵＮＩＸにおけるリモートログインのためのrsh/rloginなどｒ系コマンドプロセスに対するセキュリティパッケージであり、インターネット・ドラフトとして検討されている。認証処理に関する部分を以下に示すが、基本的には共通鍵暗号と公開鍵暗号を併用したチャレンジ・レスポンス認証方式である。

【００２８】第６図は、クライアントＡがサーバＢにログインする際のシーケンスである。同図において、共通鍵暗号（ＤＥＳ、ＩＤＥＡ等）用のセッション鍵を共有するためのフェーズ（㉑、㉓）と認証処理を行うフェーズ（㉔、㉕、㉖）に分かれている。処理シーケンスは次のようである。

①クライアントＡはサーバＢにログイン要求を送る。

【００２９】㉑このログイン要求に基づき、サーバＢはセッション鍵共有のため自身の公開鍵、乱数等をクライアントＡに送る。

③クライアントＡはセッション鍵を生成し、それをサーバＢの公開鍵で暗号化してＢに送る。サーバＢがこれを受信した時点で、クライアントＡとこの間にセッション鍵を共有できたことになるので、㉔以降、ＡＢ間のメッセージは全てこのセッション鍵で暗号化してやり取りされる。

【００３０】④クライアントＡは、自身の公開鍵、ユーザ名をサーバＢに送る。

⑤サーバＢは、クライアントＡの公開鍵とユーザ名とが登録されていることを確認の上、認証のためのチャレンジ（乱数）を生成し、それをＡの公開鍵で暗号化してクライアントＡに送る。

⑥クライアントＡは上記チャレンジのハッシュ値を計算し、それをチャレンジ・レスポンスとしてサーバＢに送る。

【００３１】⑦サーバＢは、⑥で受けたチャレンジ・レスポンスの値と保存してあったクライアントＡ向けチャレンジのハッシュ値とを比較し、それが同値であればＡのログインを許可し、異なっていればログインを拒否する。ＳＳＨ方式の長所は、チャレンジ・データが毎回変化するので、第三者が⑥のメッセージを盗聴しても再利用による「成りすまし」が不可能であるというものであるが、短所として、

・サーバＢの管理者自身が悪意でクライアントＡの公開鍵情報を書き換えることにより、クライアントＡになりすまして不正を行うことが可能である、ということが指摘されている。

（４）ＰＲＣ認証方式

このＰＲＣ(Remote Procedure Call)認証方式は、ＵＮＩＸの分散環境システムでよく用いられる遠隔手続き呼び出し機能であり、セキュリティ機能としてユーザ認証機能が用意されている。

【００３２】このＲＰＣ認証は、ＲＰＣ手続きの発行者が誰であるか（エンティティ認証機能）、そしてその発行者の権限はどのくらいであるか等をサーバが確認する機能を備えている。このＰＲＣ認証が持つエンティティ認証機能の概要は第７図のようであり、その手順の概略を述べる。

①通信に先立ち、まずクライアントとサーバはＤＥＳ暗号に用いる共通鍵（K_{ab}）をＤＨ法（Diffie-Hellman型公開鍵配送法）により共有する。ＵＮＩＸの世界では、ＤＨ法に用いる公開鍵と秘密鍵とは、ＮＩＳ(Network Information Service)によって管理され、各ユーザは通信に先立ってこのＮＩＳから予め登録してある通信相手の

公開鍵と自身の秘密鍵とを入手し、それから共有鍵（ＤＥＳ鍵）を計算により得る。

【００３３】②のクライアントでは、次の手順で認証情報を作成しサーバに送信する。（Ｉ）送信者を表す文字列（ネットネームと呼ばれる）を生成する。ＵＮＩＸの場合、

ｕｎｉｘ．＜ユーザｉｄ＞@＜ホスト・アドレス＞

という形式を有する。

【００３４】（ＩＩ）セッション鍵（乱数：Ｋ）を生成する。

（ＩＩＩ）タイムスタンプ（現在時刻：Ｔ）をセッション鍵（Ｋ）でＤＥＳ暗号化する（Ｔｅ）。

（ＩＶ）セッション鍵（Ｋ）を共有鍵（K_{ab}）でＤＥＳ暗号化する（K_e）。認証情報として（Ｉ）のネットネーム、（ＩＩＩ）の暗号化されたタイムスタンプ（T_e）、（ＩＶ）のセッション鍵（K_e）等をサーバに送信する。

【００３５】③サーバは、受信した認証情報の中の暗号化されたタイムスタンプ（T_e）を復号化し（Ｔ）、それを現在時刻と比較することによりネットネームの正当性を検証する。即ち、Ｔと現在時刻との差が許容範囲内であればそのネットネームのアクセス要求を許可するが、許容範囲外であれば拒否する。ＲＰＣ認証方式の長所として、クライアントおよびサーバの各々が自身の秘密鍵を厳密に保持し、且つ正当な相手の公開鍵を確実に得ることができれば、第３者による「なりすまし」は一般的に困難といわれているが、一定時間内であれば盗聴した認証情報をそのまま再利用すること（リプレイ攻撃）で「なりすまし」が可能であるとの短所も有する。

（５）Kerberos(RFC1510)方式

Kerberosは、ＭＩＴのAthenaプロジェクトで開発された利用者認証システムであり、１９７８年にR.NeedhamとM.Schroederによって提案された「信頼された第三者期間による認証方式」に基づいている。ＯＳＦ（オープン・ソフトウェア財団）が定めた分散処理環境構築のためのソフトウェア・パッケージであるＤＣＥ(Distributed Computing Environment)における認証サービスとして、このKerberosが採用された。

【００３６】この方式では、通信の秘匿やユーザ認証など全て共通鍵暗号方式（ＤＥＳ）のみで実現している。各ユーザの鍵を知っているのは各ユーザ自身と認証サーバだけであることを前提に、お互いの正当性を認証サーバで保証してもらうという方式を採用している。

【００３７】認証サーバにあたる部分をKerberosサーバとＴＧＳ（Ticket Granting Server：チケット発行サーバ）に分けて利用者のパスワードや鍵が利用者側のシステム（セキュリティレベルが低い）上に長時間保持されないように工夫している。また、チケット(Ticket)とオーセンディケータ(Authenticator)という考えを導入して、さらに安全性を高めている。Kerberosの認証方式を第８図に示す。

【００３８】Kerberosの認証方式は、各サーバ、利用者ＷＳ間のやりとりは全て暗号化され、さらに暗号化鍵は毎回乱数により発生しているため盗聴に強い点、目的サーバは利用者個々のユーザＩＤやパスワードを管理する必要は無く、それらはKerberosサーバだけが知っていればよい等が長所として指摘されているが、

・一定時間内であれば盗聴した認証情報をそのまま再利用し（リプレイ攻撃）可能。

【００３９】・米国における暗号製品の輸出制限のため、暗号アルゴリズムとしてのＤＥＳが実装されたKerberos製品は、日本で利用できない場合がある。

・認証サーバが各利用者の認証情報や暗号化鍵を集中管理するので、悪意の第三者がこの認証サーバへの侵入に成功するとその管理対称ドメインが全滅する。

・全てのマシン、アプリケーションはKerberos対応が必要で、導入の手間が大きい、等の短所も指摘されている。

（６）ゼロ知識対話証明方式

この方式は、１９８５年、ＭＩＴのGoldwasser,Micaliおよびトロント大学のRackoffにより提案されたもので、ある情報を持っていることをその内容を相手に示すことなく相手に納得させる方式であり、例えば、パスワードを提示することなく真のパスワードを知っていることを相手に証明できる等が利用例である。１９８６年にFiatとShamirによりファイアット・シャミア法が提案され、米国特許４，７４８，６６８号（特開平６３－１０１９８７号）。

【００４０】クライアントＡ（証明者）がサーバＢ（検証者）へ秘密の情報Ｔ（パスワード等）を転送する場合のゼロ知識対話証明方式によるシーケンスを第９図に示す。ここで、ＡはＺ＝Ｔ^2 ｍｏｄ　ｎを完全に知り、ＢはＺとｎのみを知っているとする。ここで、ｎは大きな素数ｐ，ｑの合成数である。この場合、Ｂはｎを素因数分解できなければＴを得ることが極めて困難である。

【００４１】以下の①～④をｋ回繰り返し（対話の所以）Ａの正当性を検証する。

①Ａは乱数Ｒを選び、Ｘ＝Ｒ^2 ｍｏｄ　ｎを計算し、ＸをＢに送る。

②Ｂはｂ∈｛０，１｝をℤ者択一的にランダムに選び、ｂをＡに送る。

③Ａは、Ｙ（Ｙとは、ｂ＝０の場合はＲであり、ｂ＝１の場合はＴＲ　ｍｏｄｎである）をＢに送る。

【００４２】④Ｂは、

Ｘ＝　Ｙ^2 ｍｏｄ　ｎ　　ｂ＝０の場合

ＺＸ＝Ｙ^2 ｍｏｄ　ｎ　　ｂ＝１の場合

が成立するかを検査し、これらが成り立てば検査ＯＫとする。ここで、③及び④でｂ＝０およびｂ＝１の場合に分けているのは、Ａになりすました悪意のクライアントＡ′はＴの値を知らなくても次のようにして検査に合格できるからである。即ち、常にｂ＝１であるなら、Ａは

①でＹの値として適当なＹ′を定め、Ｘ＝（Ｙ）^{2}／Ｚ　ｍｏｄ　ｎを計算し、このＸをＢに送る。次に③でＹ＝Ｙ′の値を送ると④の検査は当然合格する。また、この方式では、ｂの値を予想してから検査式を満たすＸとＹを計算できるので繰り返し１回当たりのなりすまし確率は１／２である。従ってこの手順をｋ回繰り返すとなりすまし確率を2^{-k}にできる。

【００４３】この方式の長所は、事前に秘密の認証情報ＴをサーバＢに教える必要がないので、サーバＢの正当な管理者であってもクライアントＡに成りすますことができないことであり、対話シーケンスが冗長である点、認証プロセスが複雑であり、パフォーマンスと認証精度がトレード・オフの関係となる点などが短所である。

〈生体特徴利用〉次ぎに生体特徴（個人属性）を利用した従来のセキュリティについて説明する。

【００４４】この手法は、本人の身体的、行動的特徴を認証情報として利用し、端末利用者の正当性を確認する技法である。身体的、行動的特徴としては次のようなものがある。

・身体的特徴

指紋、音声スペクトル、顔のパターン、手形、網膜パターン、耳の形

・行動的特徴

署名、筆記パターン、キーストローク

この方式は、本人にしか持ち得ない唯一の個人属性を認証情報として使用するので、認証が成功した場合の本人識別精度は高いが、正当な本人であるにも係わらず認証が失敗する等、認識確度が１００％ではなく、技術的な改善の余地があり、端末による利用者の認証等、オフライン認証（ローカル認証）では極めて有効であるが、ネットワークをまたがった認証（リモート認証）では盗聴により認証情報を再利用（リプレイ攻撃等）即ち「なりすまし」が可能となるなどの欠点がある。

【００４５】所有物利用によるセキュリティについて説明する。

〈所有物利用〉ある特定の物体が認証情報を保持しており、認証する側ではその認証情報を検証することにより、その物体を保持する人間やその物体に認証された人間、或いはその物体と連動して作動するソフトウエアやハードウエア等を正当なエンティティとして認証する。

【００４６】所有物の例としては次のようなものがある。

・鍵、トークン、パッチ

・電子キー

・磁気カード

・ＩＣカード

・非接触型カード（光式、電磁波式などＩＣカードの発展型と言える）

例えば、端末のロックを解除するための鍵やトークン、電子キーを所持する人間は、その端末の正当な利用者として認証される。

【００４７】しかし、これらの所有物の紛失や盗難による悪用を防止するため、ネットワークを介した認証では、磁気カードのように所有物でまず利用者識別を行い、更にサーバ（アクセス先のホストコンピュータ等）による暗証番号の検証により利用者の正当性を確認する等、「知識利用」の技法と組み合わせて用いられることが多い。

【００４８】ＩＣカードではこれがさらに発展し、まずＩＣカード自身がＩＣカードを使用しようとしている人間を暗証番号で検証し、これが成功して初めてネットワークを介したサーバとの認証動作に入る。サーバによるＩＣカード（即ちＩＣカードにより検証された人間等のエンティティ）認証処理は「知識利用」や「暗号利用」の技法を利用して行われる。

【００４９】この手法は、所有物を厳密に保持すれば第三者による「なりすまし」は一般に困難である点、ＩＣカードは通常、耐タンパー性（Tamper　Free）を有しており、外部からメモリ内の情報を読み書き不可能な構成となっている。そのため暗号鍵やパスワード等個人に依存した情報を比較的安全に格納、管理できる点、またセキュリティ処理機能そのものをＩＣカード内に組み込むことにより、さらに安全な認証通信が可能となる点などが長所である反面、所有物利用による認証システムでは、大抵の場合、その所有物とクライアントとなる端末との間に専用の入出力機器が必要である点、磁気カード、ＩＣカード等でネットワークを介した認証処理の場合、認証シーケンスそのものは結局「知識利用」や「暗号利用」の技法を使用しているため、当然であるがそれらに特有の短所も付随することになる点などが短所として指摘されている。

【００５０】

【発明が解決しようとする課題】上述のように、従来の各種エンティティ認証方式は長所を有する反面、短所も有する。ところで、エンティティ認証が想定する直接の脅威は、パスワード等の不正入手による「なりすまし」であるが、この「なりすまし」が一旦成功し、システムに侵入されると、データの改ざんやファイル破壊、不正データの生成等様々な不正行為の脅威にさらされることになる。また、このような脅威は外部からの不正アクセスによるもののみならず、システム管理者等の内部犯罪によって引き起こされる可能性もある。

【００５１】従って、アクセスされる側のシステムにとってアクセスしてくる実体が何であるかを確認するエンティティ認証は、セキュリティ上の脅威に対する最前線の防衛網と言え、その重要度はシステムの機密度に応じて大きくなる。ここで今まで述べてきたエンティティ認証方式の「なりすまし」に対する強度を外部および内部の不正エンティティに対してまとめてみると第１０図のようになる。

【００５２】上記いずれの方式も欠点はあるものの、システムの環境、構成によっては十分実用的なものである。しかしながら、第１０図に示すようにシステム管理者等のシステムに精通した人間の悪意の内部犯罪による脅威に対しては防衛できないものがほとんどであり、たとえ防衛できる方式であっても認証処理が複雑になるなどの欠点がある。

【００５３】以上で述べたように、エンティティ認証はセキュリティ上の様々な脅威に対する最前線の防衛機能であるが、インターネット時代においては、その適用領域の広範さと相互接続性の観点から、導入が簡単で、従って仕組みが簡単で、且つ脅威に対して十分有効な方式である事が望まれる。そこで、上述の各種認証方式の長所、短所に対する検討を踏まえ、新たな認証方式に要求される事項をまとめると次のようになる。

（１）盗聴等によって盗まれた認証情報が第三者によって再利用できないこと。

【００５４】例えば、ワンタイム・パスワード方式（S/Key等）はこの用件を満たしているが、デジタル署名付認証トークン方式はそのタイムスタンプの許容時間内であれば盗聴トークンが再利用出来てしまう。

（２）認証サーバに認証情報が保存されないこと。換言すれば、認証サーバは利用者個々の認証情報を保管する必要がなく、ただログイン時の認証情報が正当か否かを識別できる機能を有すればよい。これによって、たとえ悪意の第三者が認証サーバに侵入できたとしても利用者個々の認証情報を得ることは出来ない。

（３）認証シーケンスは極力簡単であること。

【００５５】これにより、システムに対する負荷を最小限にし動作の安定性を得る。従って、チャレンジ・レスポンス方式やゼロ知識対話証明方式のような対話シーケンスを用いない。

（４）認証情報は毎回異なり、しかもその情報は無限に存在すること。これにより（１）の用件を満足しつつ、既存ワンタイム・パスワード方式（S/Key等）のようにパスワードを使い切った場合に再度初期情報をサーバに再登録するといった定期作業が不要となる。

（５）生体特徴利用のような特殊外部測定機器を必要としないこと。

【００５６】特殊な機器はインターネットを介した相互運用性を損ない、また導入コストの高騰につながるので、このような外部機器は用いない。かくして、本発明は、簡単な手順による認証方法を用い、たとえ認証情報などが盗まれても盗まれた認証情報などの第三者による再利用が困難な認証方法、認証装置、認証サーバ等を提供することを目的とする。

【００５７】

【課題を解決するための手段】上記課題を達成するための本発明の、認証要求者からの認証の要求に対して、公開鍵暗号方式により認証者が認証要求者を認証する方法は、前もって認証者は、認証要求者の認証情報を検査するための第１の検査情報を保存しておく保存工程と、前記認証要求者は前記認証者に認証要求を送る認証要求送出工程と、前記認証者は、前記認証要求者から送られてきた認証要求に対して、認証情報要求を前記認証者に送ることによって応る認証情報要求工程と、前記認証要求者は、前記認証情報要求に応答して、認証情報を生成するために前記認証要求者が自身が保持している第１の種情報を前記認証要求者の秘密鍵を用いて暗号化して生成した第１の認証情報を前記認証者に送るとともに、生成した前記第１の認証情報を次回の認証要求のための第２の種情報として前記保持していた第１の種情報に換えて保存する認証情報送出工程と、前記認証者は、前記認証要求者から送られてきた前記第１の認証情報を前記認証要求者の公開鍵によって復号化することにより、第２の検査情報を生成し、この第２の検査情報を前記前もって保存していた前記第１の検査情報と比較する比較工程と、前記認証者は、前記第２の検査情報が前記第１の検査情報と一致した場合には、前記認証要求を許可する旨を前記認証要求者に通知すると共に、前記第１の検査情報に代えて前記第２の検査情報を保存する更新工程とを具備することを特徴とする。

【００５８】この認証方法によると、認証要求者は認証情報を生成するための種情報（前回ログイン時に使用した認証情報）を自身の秘密鍵で暗号化したものを認証情報として認証者に送り、認証者は認証要求者から受信した認証情報を認証要求者の公開鍵で復号化し、認証側で保存してあった認証情報の検査情報（前回ログイン時に使用した認証情報）と比較し、それらが同一か否かを検査することにより認証処理が達成される。

【００５９】従って、認証要求者が自身の秘密鍵を厳格に保管している限り、認証要求者側で保存している種情報および認証者側で保存している検査情報を第３者が知り得ても、彼は認証情報を生成することはできないので、その第３者による「なりすまし」は不可能である。また、認証者側では、認証要求者から受信した認証情報を認証要求者の公開鍵で複合し、認証者側で保存してあった認証情報検査情報（前回のログイン時に使用した認証情報）と比較し、それらが同一であれば、即座にその認証情報を次回の認証情報検査情報として保存するので、第３者が送信中の認証情報を盗聴し、それをそのまま再利用して認証要求者に成り済ますことが可能となるタイムラグは実質的に零であり、不可能である。

【００６０】この認証方法を適用するために、本発明にかかる、複数の認証要求者からの認証要求に対して認証を与えるための認証情報を保存する認証情報ファイルサーバは、認証要求者毎に認証要求者の認証情報を検査するための検査情報を記憶する手段と、任意の認証要求者からの認証要求を受けると、認証情報要求メッセージをその認証者に送る手段と、その認証要求者から送られて

きた認証情報を、その認証要求者の公開鍵によって復号化して、新たに検査情報を生成し、この新たに生成した検査情報を前記前もって保存していた検査情報と比較する手段と、前記新たに生成した検査情報が前記保存していた検査情報と一致した場合に、前記認証要求を許可すると共に、前記保存していた検査情報に代えて前記新たに生成した検査情報を保存する手段とを具備する。

【００６１】また、上記認証方法に好適な本発明の、外部の認証サーバの支援により、認証要求者からの認証要求に対する認証を与える認証装置は、前記認証要求者を認証する認証情報を生成するための種情報を記憶する記憶手段と、前記認証サーバに認証要求メッセージを送ると共に、この認証要求メッセージに応答する前記認証サーバからの認証情報要求メッセージを受ける送受信手段と、認証サーバからの認証情報要求メッセージに対して、前記記憶手段に記憶している前記種情報を秘密鍵を用いて暗号化することにより認証情報を生成する暗号化手段と、生成した認証情報を前記認証サーバに送ると共に、前記記憶手段において、記憶されている前記種情報に換えてこの生成された認証情報を記憶する認証送出手段とを具備する。

【００６２】また、特に、不特定のユーザが使用可能な端末装置において、特定の認証要求者による認証要求に対してはセキュリティの高い本発明の、外部の認証サーバの支援により、認証要求者からの記憶媒体を介した認証要求に対して認証を与える認証端末装置は、本体と、認証要求者を認証する認証情報を生成するための種情報とその認証要求者についての秘密鍵と前記種情報から前記秘密鍵を用いて認証情報を生成するプログラムとを記憶する記憶媒体を受け容れるためのインタフェース手段とを有し、前記本体は、前記認証要求者からの認証要求を受ける受信手段と、この認証要求に応答して前記認証サーバに認証要求メッセージを送ると共に、この認証要求に応答する前記認証サーバからの認証情報要求メッセージを受ける要求手段と、認証情報要求メッセージに応答して、前記インタフェース手段を介して、前記記憶媒体中のプログラムを実行させる指令手段であって、前記プログラムに対して、前記種情報から前記秘密鍵を用いてこの認証要求者の認証情報を生成せしめ、生成した認証情報を前記インタフェース手段を介して前記本体に送り返せしめると共に、この生成した認証情報により前記記憶媒体中の前記種情報を更新せしめる指令手段と、送り返された認証情報を前記認証サーバに送る手段とを具備することを特徴とする。

【００６３】また、本発明は、上記認証方法を適用するうえで、認証要求者側が使用する装置に用いられるプログラムを記憶する記憶媒体にも適用可能である。かかる、本発明の、外部の認証サーバの支援により、認証要求者からの認証要求に対する認証を与える認証プログラムを記憶する記憶媒体は、前記認証プログラムは、前記認証要求者を認証する認証情報を生成するための種情報を所定の記憶手段に記憶させる第１のプログラムコードと、前記認証サーバに認証要求メッセージを送る第２のプログラムコードと、前記認証サーバからの認証要求メッセージを受け取る第３のプログラムコードと、認証情報要求メッセージに対して、前記記憶手段に記憶している前記種情報から秘密鍵を用いて認証情報を生成する第４のプログラムコードと、生成した認証情報を前記認証サーバに送ると共に、前記古い種情報に換えて、この生成した認証情報を新たな種情報として記憶する第５のプログラムコードとを具備することを特徴とする。

【００６４】本発明の好適な一態様に拠れば、認証要求を許可する旨の通知を受けた場合に、種情報の更新を行い、通知を受けなかった場合には、更新を行わないことを特徴とする。認証要求者側の種情報と認証者側の検査情報の同一性を担保するためである。本発明の好適な一態様に拠れば、前記第１の種情報の初期値として前記認証要求者の識別情報を用いる。

【００６５】本発明の好適な一態様に拠れば、認証情報を認証要求者の公開鍵証明書付きで認証サーバに送ることを特徴とする。認証者側での認証要求者の公開鍵の取得が容易且つ確実となる。本発明の好適な一態様に拠れば、前記記憶手段は、認証要求者毎の公開鍵証明書を検査情報と共に記憶する。次回のログイン時には、公開鍵証明書を送る必要がなくなる。

【００６６】本発明の好適な一態様に拠れば、認証者において検査情報同士が一致しなかった場合には認証要求を拒否する。本発明の好適な一態様に拠れば、前記認証要求者の秘密鍵は、真正の持ち主のみが復号化できるように暗号化されていることを特徴とする。秘密鍵が守られる。

【００６７】本発明の好適な一態様に拠れば、前記記憶媒体はＩＣカードである。本発明の好適な一態様に拠れば、前記記憶媒体はパスワードを更に記憶し、更に、前記認証要求者から入力されたパスワードと前記記憶媒体に記憶されたパスワードとを比較し、一致したときにのみ、前記記憶媒体は認証情報を前記本体に送り返す。

【００６８】本発明の好適な一態様に拠れば、秘密鍵を用いた種情報から認証情報への変換は記憶媒体においてのみ行われ、前記秘密鍵は前記本体側に送られないようにされる。重要な秘密鍵は記憶媒体外に出ることはない。

【００６９】

【実施の形態】以下添付図面を参照しながら、本発明の好適な実施形態乃至実施例を説明する。第１１図は本発明にかかる方式が適用されるネットワークの構成を示すこのネットワークでは、複数のクライアント２００，３００…がインターネットによって接続されている。また、このネットワークに認証サーバ１００も接続されている。

【００７０】クライアント２００がクライアント３００と通信するときは、クライアント２００が認証要求者となり、クライアント３００が認証者となる。本実施形態では、認証者をサーバと呼ぶ。認証サーバ１００は、複数のクライアントからアクセス可能なデータベースを有するものので、それらクライアントからの認証要求を受けて認証を行うもので、認証サーバと呼ぶ。第１２図を参照。即ち、クライアントとクライアントとが通信を行うときは、一方がサーバとして振る舞う。

【００７１】本実施形態の認証方法は、本質的には認証局（ＣＡ）の存在を前提としない。クライアントとクライアント間のデータの送受は、認証局（ＣＡ）の介在を必要としなくて直接行われることもあり、認証サーバ１００（例えば、ＣＡ等）を介して行う場合もある。認証者も認証要求者も、人そのものではなく、オペレータ或いはユーザの行為を媒介にして動作するコンピュータ（或いはシステム）である。

【００７２】第１３図は、認証要求者としてのクライアントＸと認証者として認証サーバＹとの単純化した構成からなるネットワーク（第１１図）における、本発明を適用した認証アルゴリズムの例を示す。第１３図の例では、前提として、公開鍵暗号アルゴリズムを使用する。クライアントＸは自身の秘密鍵K_Sを、またサーバＹは、そのクライアントの秘密鍵K_Sに対応する公開鍵K_P、並びにその公開鍵の証明書C_{K_P}を保持しているものとする。また、S_dは公開鍵暗号アルゴリズムの暗号化関数、S_dは公開鍵暗号アルゴリズムの復号化関数を意味する。

【００７３】本システムでは、第１３図に示すように、クライアント側は認証情報生成種データファイル２０４を有し、サーバ側はクライアント認証情報検査データファイル１０５を有する。認証情報生成種データファイル２０４は、認証情報を生成するための種となるデータを記憶するファイルである。ここで、本システムでは、「認証情報」は、認証要求者が認証者に認証を要求するために認証要求者が認証者に送る情報を意味し、クライアント側において種データから生成される。この入出力情報はサーバ側において、サーバが有するそのクライアントの検査で田堵照合し、照合がとれれば、そのクライアントを真正な認証要求者と見なすというものである。

【００７４】第１４図は、サーバＹが有する認証情報検査データファイルの構成を有する。即ち、サーバＹは、各クライアント毎に、「認証情報検査データＤ」と「公開鍵K_P」と「公開鍵証明書C_{K_P}」とを有する。第１４図の例では、サーバＹは、クライアントＸについて検査データD_Xと公開鍵K_{PX}とを有し、クライアントＷについて検査データD_Wと公開鍵K_{PW}とを有する。

【００７５】第１５図は、本実施形態の認証を実現するために、クライアントＸ及びサーバＹそれぞれにおける処理手順と、これらの間で行われる連絡の手順を示す。第１３図及び第１５図に従って、本実施形態の手順を、クライアントＸがサーバにログインする際の認証を受けようとする場合について説明する。

〈初期情報の登録〉本実施形態では、ログインに先立って、クライアントは初期種データD_{50}を設定し、サーバＹにおいて初期検査データD_{50}を初期的に登録することが必要である。これらの登録は、最初に一回だけ行えば良く、一旦行ってしまえば、その後に登録することは不要である。

【００７６】この登録作業は、クライアント側ではクライアント自身が行い、サーバ側においては一般的にクライアントのアクセス権限の設定等を伴うので相応の権限を持ったシステム管理者が行うことが好ましい。初期種データD_{50}は、乱数やクライアントのE-mailアドレスや利用者識別名等何でもよい。また、秘密鍵K_Sさえ秘密に保たれているならば、初期種データD_{50}を特に秘密にしておく必要もない、登録後は、登録された旨がクライアントに通知される。

【００７７】後述するように、種データＤはクライアントにおいて認証情報の生成のために使われる。そして、その認証情報を用いた認証要求が一旦受け入れられると、生成された認証情報は次のログインのための認証要求のための認証情報生成用の種データとして記憶される。また、サーバ側では、受信した認証情報と前もって保存している検査データＤとを比較して照合が得られたならば、その受信した認証情報を、そのクライアントからの次のログインのための検査データとして保存する。従って、本システムでは、認証情報生成種データファイル２０４に記憶されている種データと、サーバ側の検査データファイル１０５に記憶されている検査データとは値として一致しているので、第１３図においては、便宜上、D_{n-1}として表している。種データや検査データを一般的にD_{n-1}と表したのはそれらのデータが前回のログインにおいて生成されたものであるからである。

【００７８】第１３図の例では、クライアントＸの初期種データはD_{50}として登録されている。本実施形態の認証プロトコルは、クライアントＸは、始めての認証が許可された場合には、認証情報をこの初期種データD_{50}から生成する。認証のためのセッションが終了する毎に、今まで保存していた種データD_{n-1}をクライアントＸの秘密鍵K_Sで暗号化し、それを次回の認証セッションのための種データD_nとして保存する点に大きな特徴がある。尚、前回の種データD_{n-1}は次回以降のログインでは使用されることはないが、履歴の保持のために保存しておいても良い。

【００７９】以下、順に、第１３図および第１５図に則して、本実施形態の処理手順を説明する。

・ステップ①

本実施形態では、認証はログインを行おうとするクライアントが真正なクライアントであるか否かを認証するも

のである。従って、認証に先立ってサーバへのログインが行われる。本実施形態でのログインは、利用者識別名（User-id等）をサーバYに送ることによって行われる。このログインメッセージは平文のままでも、暗号文の形式でも良い。

【００８０】・ステップ②

ログインメッセージを受け取ったサーバYは、クライアントXに対して認証情報要求メッセージを送る。

・ステップ③

この認証情報要求メッセージを受け取ったクライアントXは、サーバに返すべき認証情報として、自身が保存している種データDを自身の秘密鍵K_Sで暗号化してサーバYに送る。

【００８１】第１３図の例は、初期登録後の始めて認証セッションの開始であるので、種データはD_{S0}であり、従って、データD_{S0}をクライアントXの秘密鍵K_Sで暗号化したものD_1がサーバYに送られる。

・ステップ④

サーバYは、クライアントXから認証情報D_1を受信すると、既に得ているクライアントXの公開鍵K_Pで復号化する。前述したように、本実施形態の認証情報D_nは公開鍵暗号化アルゴリズムに従って暗号化されている。即ち、クライアントXを表す筈の認証情報D_1が、クライアントXの真正な種データD_{S0}をそのクライアントXの秘密鍵K_Sによって暗号化されたものであれば、その認証情報D_1を公開鍵K_Pによって復号化したものは、公開鍵暗号化アルゴリズムに従えば、クライアントXの秘密鍵K_Sによって暗号化される前の種データD_{S0}に一致するはずである。

【００８２】・ステップ⑤

それで、サーバYは、復号化して得た情報D_{S0}と、ファイル１０５から読み出したところのクライアントXの検査データD_{S0}とを比較照合する。

・ステップ⑥

サーバは照合結果をクライアントに返す。

【００８３】前述したように、照合が一致した場合は、認証を要求したクライアントXは真正なクライアントであることを意味するから、ログインを許可する旨のメッセージを返す。また、次回のクライアントXからのログイン要求に備えて、クライアントXから受け取ったところの暗号化されている認証情報D_1をファイル１０５内に保存する。サーバYにおけるこの認証情報の更新（上書き保存）は、ステップ⑤における比較結果が一致したときのみ行われる。ファイル１０５内に書き込まれた暗号化認証情報D_1はファイル１０５内では次回のログインのための検査データとして記憶される。

【００８４】・ステップS⑦

サーバからの認証処理結果を受けたクライアントでは、その認証処理結果が許可かまたは拒否であるかを判断する。

・ステップS⑧

認証が許可されたものであった場合には、サーバ側に送っていた認証情報D_1を次回のログイン時の種データD_1としてファイル２０４に記憶する。

【００８５】認証が拒否されたものであった場合（処理結果が所定時間以内に返ってこなかった場合も含む）には、認証情報D_1を次回のログイン時の種データD_1として使うことはできないので、破棄する。換言すれば、ログインを再試行する場合には、クライアントは種データD_{S0}から認証情報D_1を再度生成する。以上が、始めてログインが行われたときにおける、ログイン要求に対する認証のための処理手順である。

【００８６】次回にログインが行われたときには、ステップ①～⑧が繰り返される。即ち、第１３図に示すように、クライアントXは、サーバYからの２回目の認証情報要求に対しては、保存しておいた種データD_1を認証情報としてその秘密鍵K_Sで暗号化して生成し、この暗号化した認証情報D_2をサーバYに送る。サーバYは送られてきた認証情報D_2を公開鍵K_Pで復号化して検査データD_1を生成し、この検査データD_1を格納しておいた検査データD_1と比較する。比較の一致がとれれば、ログインを許可する点では、第一回目のログイン時と同じである。

【００８７】この方式は、一回に限り有効な認証情報を無限に生成できるので、以降これを『無限ワンタイム認証方式』と呼ぶことにする。この無限ワンタイム認証方式の従来方式に比べ特に強調されるべき利点は次のようである。

（１）次回ログイン時に生成される認証情報は、正当な認証要求者のみが彼の保持する秘密鍵を用いて生成することができるのであり、外部の第三者盗聴者のみならず、サーバの認証情報管理者でさえ、その次回のための認証情報を知ることが出来ない。このことにより、サーバ側の内部悪意者による利用者への「なりすまし」による不正行為、即ち内部犯罪をも防ぐことが可能である。

【００８８】即ち、認証要求者は、生成種データ（前回ログイン時に使用した認証情報）を自身の秘密鍵で暗号化したものを、認証情報として認証者に送り、認証者は認証要求者から受信した認証情報をその認証要求者の公開鍵で復号化し、認証者側で保存していた検査データと比較して一致したときのみ、認証要求に対して許可を行う。従って、自身の秘密鍵を厳格に保管している限り、認証情報、検査データ、認証情報生成種データのいずれか（或いは全て）が第３者に知られることとなっても、その第３者による当該クライアントのなりすましは不可能である。

【００８９】さらに、認証者では、１つの認証要求処理プロセスにおいて、検査データ同士の比較を行い、一致しないことが或いは一致したことが確認されるまではその処理プロセスから抜けることはなく、また、一致がと

れれば直ちに、検査データの更新を行うので、検査データの更新までのタイムラグは実質的に零であり、従って、第３者が、送信中の認証情報を盗聴し、それをそのまま再利用して認証要求者に成り済ますことの猶予時間は実質的に零である。

（２）認証情報の登録は一回限りで済み、一旦、登録を行えば、クライアントは無限にセキュリティの高い認証情報を生成することが出来る。但し、秘密鍵、公開鍵のペアーを変更した場合は、再度、サーバに登録する必要がある。

（３）クライアントーサーバ間の認証処理は対話シーケンスを持たず、ログイン時に１メッセージ（認証情報）を送信するのみである。従って、サーバ側及びクライアント側で必要とされるプログラムは極めて簡単なものとなる。

（４）クライアント側で認証情報をサーバ側に送ってから、その認証情報を次の認証情報に更新する（即ち、D_nからD_{n+1}に更新）迄の時間間隔が零に等しい。したがって、たとえ通信中に認証情報が盗聴されても、盗聴者がそれを再利用し得る時間的隙間が皆無である。

【００９０】これに対し、既存方式で認証情報の一部にタイムスタンプを用いるような方式では、サーバ側で一定の時間許容範囲を設けているため、認証情報を盗聴後即時にその許容範囲時間内で再使用すれば真のクライアントに成りすましてサーバにログインできる（リプレイ攻撃）タイミングが存在し得るが、本方式ではこれが不可能である。

（５）サーバ側において、検査データD_nをサーバ管理者などの内部関係者が盗用し、偽りの認証を試みたとしても、これらの者が用いたD_nは、認証プロセスの中で真正な認証要求者の公開鍵により複合化され生成されたD_{n-1}と比較されるので、認証が成功することはない。即ち、サーバの認証情報を知ることができる内部関係者であっても、真正な認証要求者に成りすますことはできないのである。

【００９１】

【実施例】上述の無限ワンタイム認証方式を具体化した実施例を以下に説明する。第１６図は、この実施例のためのサーバ側構成を示す。このサーバは、ＯＳ１０１として、例えばWINDOWSまたはMAC OSまたはUNIXまたはNETWAREを用いる。ネットワーク１０２との通信プロトコルは例えば、ＴＣＰ／ＩＰやＯＳＩやNETWAREを用いる。

【００９２】検査データファイル１０５は第１４図に関連して説明したファイルの構成を有し、具体的には、クライアントの識別名情報Ｘと、検査データD_{n-1}、公開鍵証明書$C_{K_{PX}}$とを記憶する。公開鍵証明書$C_{K_{PX}}$は、バージョン番号、シリアル番号、発行局名、証明書の有効期限、ユーザ識別子、公開鍵と関連情報等を含む。公開鍵ファイル１０７は、証明機関ＣＡの公開鍵K_{pc}を保存する。この公開鍵K_{pc}はクライアントＸの公開鍵証明書に付されているディジタル署名を検査するのに使用する。

【００９３】復号処理プログラム１０６は、クライアントＸの公開鍵証明書$C_{K_{PX}}$の検査を行うことによりKPxを得、受信した認証情報D_n（クライアントの秘密鍵K_Sで暗号化されている）を公開鍵K_{Px}で復号化して検査データD_{n-1}を生成する。第１７図はクライアント側の構成を示す。このクライアントシステムは、ＳＹＳ２０１として、例えばWINDOWSまたはMAC OSまたはUNIXまたはNETWAREを用いる。通信プロトコルは例えばＴＣＰ／ＩＰやＯＳＩやNETWAREを用いる。この場合、クライアント側の通信プロトコルはサーバ側の通信プロトコルに一致させる必要がある。しかし、クライアント側のＯＳはサーバ側のＯＳに一致させる必要はない。秘密鍵ファイル２０６は、当該クライアントＸの秘密鍵K_Sを保存するファイルである。この秘密鍵K_Sは所定の暗号化手順により暗号化されていることが好ましい。

【００９４】秘密鍵K_Sの暗号化及び復号化、さらに、秘密鍵K_Sを用いた認証情報種データD_{n-1}から認証情報D_nへの暗号化は、認証処理プログラム２０２の支援の下に暗号化処理プログラム２０７によって行われる。認証情報生成種データファイル２０４はクライアントＸの認証情報生成のための種データを記憶する。

【００９５】サーバ側の認証処理プログラム１０４は第１５図の右側の制御手順を実行し、クライアント側の認証処理プログラム２０２は同図左側の制御手順を実行する。第１７図の実施例システムの特徴は、秘密鍵K_Sをクライアント側システムのローカルディスク上で暗号化して保管する点に特徴がある。これは、第１２図などで示した実施形態にかかる無限ワンタイム認証方式がクライアントＸが自身の秘密鍵K_Sを厳密に保管することが前提としているために、第１７図のクライアントシステムは、その管理機能を秘密鍵K_Sの暗号化で達成するものである。

【００９６】暗号化処理プロセス２０７は種々のものが使用可能である。例えば、第１７図システムを使用するユーザにパスワードを要求する手法も簡便であるが、ＤＥＳのような適当な共通鍵暗号方式を用い、クライアントＸのみが知るパスフレーズを鍵としてK_Sを暗号化して保管することが好ましい。この結果、K_Sが第三者に知れることがなくなり、クライアントＸになりすますことは実質上不可能となる。また、特殊機器を必要とせず暗号ソフトウェアをインストールするだけでK_Sを秘密に保管できる、また、外部インターフェイス機器が不要である等の効果を得ることができる。

【００９７】特に、暗号処理プログラム２０７をプラグインプログラムモジュール化することにより、操作性、拡張性、可変性は飛躍的に向上する。クライアントの公開鍵K_pをサーバに送る形態は種々の形態が考えられる。第１６図の例では、サーバ側は、各ログインごとに

クライアントからのクライアントＸの公開鍵証明書を得ることを前提としている。即ち、たとえば、クライアントがサーバに送る認証情報と共にクライアントＸの公開鍵証明書ＣＫ$_{PX}$を送る。

【００９８】サーバ側の認証処理プログラム１０４は、クライアントＸのログインメッセージを受信すると、クライアントに認証情報要求メッセージを返すと共に、入手した利用者Ｘの公開鍵証明書に付されている証明局ＣＡのディジタル署名を、証明局ＣＡの公開鍵Ｋ$_{PC}$（ファイル１０７中に保存されている）を用いて検査する。検査が確認されたならば、その公開鍵証明書はクライアントＸの正当な公開鍵証明書であることが確認される。また、クライアントＸの公開鍵証明書ＣＫ$_{PX}$をファイル１０５に保存する。プログラム１０６は、データファイル１０５にアクセスして、公開鍵証明書ＣＫ$_{PX}$中のクライアントＸの公開鍵Ｋ$_{PX}$を取り出す。

【００９９】〈変形例〉本発明はその趣旨を逸脱しない範囲で種々変形が可能である。

第１変形例：　たとえば、１６図の例では、クライアントの公開鍵証明書はログイン毎にクライアントからサーバ側に送信されるようにしていた。本方法では、クライアントの公開鍵は秘密にしておく必要がないので、毎回ログイン毎にクライアントＸの公開鍵証明書を送る必要はない。

【０１００】そこで、サーバ側のプログラムのログインプロセス中に、クライアントＸからのログインがあったならば、そのＸの公開鍵証明書ＣＫ$_{PX}$がすでにファイル１０５中に保管されているか否かを検査する手順を追加することを提案する。その場合、サーバ側は、公開鍵証明書が登録されていないクライアントからのログインがあった場合には、認証情報要求メッセージをそのクライアントに送る前に、公開鍵証明書要求メッセージを送るようにしてもよい。

【０１０１】第２変形例：　上記実施例は、ログインに使用するクライアント端末がＫ$_S$を保管している端末に限定されるという不便さがある。そこで、秘密鍵Ｋ$_S$をクライアント端末上ではなくＩＣカード上に保管し、クライアントＸが常時そのカードを持ち歩くことを提案する。そのためのクライアント側のシステムの構成を第１８図に示す。第１８図のシステムは、ＩＣカード３００に、ユーザのパスワードを記憶するパスワードファイル３０１と、公開鍵証明書を記憶するファイル３０２と、秘密鍵Ｋ$_S$を記憶するファイル３０４と、特に暗号処理プログラム３０４とを有する点にある。

【０１０２】第１８図に示したシステムをクライアント側構成とした場合には、サーバ側構成は第１６図構成を援用することができる。第１９図は、第１８図のクライアント側の認証処理プログラム３０８（クライアントホスト側）と暗号処理プログラム３０３（クライアントカード側）の連携動作を説明する。

【０１０３】先ず、ユーザによるログイン（例えば、ＩＣカードを不図示のカードリーダに読み込ませる）があると、暗号処理プログラム３０３は、端末の認証処理プログラム３０８を介してクライアントに対して認証情報の要求メッセージ（パスワードの要求メッセージ）を送る。ユーザが正規のユーザであるならば、正しいパスワードを、端末の不図示のキーボードなどから入力するであろう。そのパスワードが入力されると、プログラム３０８はその入力されたパスワードをインタフェースを介して暗号処理プログラム３０３に送る。暗号処理プログラム３０３は、受け取ったパスワードを、ファイル３０７中に記憶しておいたパスワードと比較する。

【０１０４】一致しなければ、その旨のメッセージを認証処理プログラム３０８に返すので、認証処理プログラム３０８は当該ログインを拒絶する。一致が得られれば、カード側の暗号処理プログラムは、クライアントに対してＩＣカードの利用許可を発行するともに、認証サーバに対して認証要求を行うことが許可されたことを通知する。

【０１０５】次に、クライアントは認証サーバに対する認証要求を行う。以後の手順は第１３図に説明した通りである。この場合、クライアント側においては、種データＤ$_{n-1}$から認証情報を生成するための秘密鍵Ｋ$_S$による暗号化は全てＩＣカード３００内の暗号処理プログラム３０３によって行われることが重要である。即ち、秘密鍵Ｋ$_S$についてのいかなる情報もホスト側に伝わることはなく、伝わるのは認証情報Ｄ$_n$である。前述したように、認証情報Ｄ$_n$は第３者によって見られてもそれを解読することはできないからである。

【０１０６】尚、第１８図のクライアント側システムでは、秘密鍵ファイル３０４が認証処理プログラム３０８に対してオープン（漏えい若しくは改ざんの虞）になることは好ましくない。クライアントのホストシステムは不特定の多数のユーザが使用する可能性があり、秘密鍵Ｋ$_S$が生の形でホストシステムに曝されるのは好ましくないからである。そこで、ファイル３０４中の秘密鍵Ｋ$_S$をパスワードファイル３０７中のパスワードによってＤＥＳなどの暗号アルゴリズムに従って暗号化することが好ましい。秘密鍵Ｋ$_S$を暗号化しておけば、ホスト中のたとえば認証処理プログラムが改ざんされて、ファイル３０４から秘密鍵Ｋ$_S$を読み出されても、ＤＥＳにより暗号化されているので、それが解読される可能性は極めて少ない。

【０１０７】この変形例によれば、Ｋ$_S$がＩＣカードに保存されるので、第三者がクライアント端末を使用してクライアントＸ本人になりすますことは不可能である。換言すれば、クライアント側のシステムは汎用パソコンであっても良く、このパソコンを、クライアントＸ本人以外の者が使用することが可能となる。また、ＩＣカードとインターフェース可能な端末であれば、どのような

端末でもクライアント側本体装置として使用可能となる。従って、例えば携帯端末で社外からリモート・ログイン等も可能となる。更に、ログイン処理実行に先立ち、ＩＣカードがクライアントＸ（利用者）を暗証番号等で認証する方式としているので、ＩＣカードを紛失しても第三取得者がクライアントＸになりすますことは困難である。

【０１０８】第３変形例：　尚、上記実施形態及び実施例さらには変形例では、クライアントの公開鍵はサーバ自身が前もって保存している、或いはサーバがクライアントから取り寄せるという形態を前提としていたが、前述したように、一旦クライアントから送られてきた彼の公開鍵をサーバ側で保管しておき、以後のログインにおいてその保管しておいた公開鍵を証明書とともに流用してもよい。公開鍵は他人に知られても構わないからである。但し、証明書は（従って公開鍵も）有効期間が設定されているから、有効期間経過後のログインに対しては、前述した手法により、公開鍵証明書を再送してもらうことが好ましい。

【０１０９】第４変形例：　また、上記実施形態及び実施例さらには変形例では、ネットワークの存在を前提としていたが、本発明はネットワークを要件としない。およそ、認証が必要であれば、例えば、ホストと入出力装置との間でも本発明を適用できる。

第５変形例：　上記実施形態では、通信回線（有線であろうが無線であろうが）を介したデータのやり取り時における認証の問題を扱ったが、本発明は、たとえば、カードを利用したドアの開閉装置に適用することも可能である。即ち、この場合は、ロック気候が認証サーバとして振る舞う。

【０１１０】

【発明の効果】以上説明したように、本発明によれば、簡単な手順による高度な認証方法、認証装置、認証サーバ等を提供することができる。即ち、検査情報および種データは毎回変更されるので、リピート攻撃に強く、また、たとえ送信中の認証情報が盗まれても、それを第３者がそのまま再利用する時間はほとんどないので、セキュリティは保たれる。さらに、たとえ、種情報、または、認証情報または検査データが盗まれても、クライアントの秘密鍵の管理が行われているかぎりは、その盗まれた認証情報を第三者が再利用することは極めて困難である。

【図面の簡単な説明】

【図１】　認証の分類を説明する図。

【図２】　従来のチャレンジ・レスポンス方式の概要を説明する図。

【図３】　公開鍵暗号方式の一般モデルを説明する図。

【図４】　従来の認証子照合法を説明する図。

【図５】　従来のディジタル証明付き認証トークン方式を説明する図。

【図６】　従来のＳＳＨ方式を説明する図。

【図７】　従来のＲＰＣ認証の概要を説明する図。

【図８】　Kerberos認証方式の概要を説明する図。

【図９】　零知識対話証明方式の概要を説明する図。

【図１０】　従来の各種セキュリティ方式の短所をまとめた図。

【図１１】　本発明の実施形態にかかる認証システムの構成を原理的に示す図。

【図１２】　本発明の実施形態にかかる認証システムの構成を原理的に示す図。

【図１３】　本発明の実施形態による認証手順の動作結果例を説明するフローチャート。

【図１４】　本発明の実施形態による認証手順を説明するフローチャート。

【図１５】　本発明の実施形態にかかる認証サーバに記憶される認証情報ファイルの構成を説明する図。

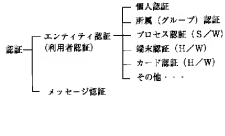
【図１６】　本発明の実施例のサーバ側のシステム構成を示す図。

【図１７】　本発明の実施例のクライアント側のシステム構成を示す図。

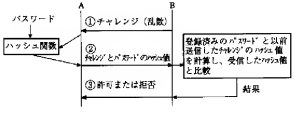
【図１８】　変形例にかかるクライアント側のシステム構成を示す図。

【図１９】　変形例にかかるクライアント側の処理手順を説明するフローチャート。

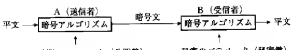
【図１】



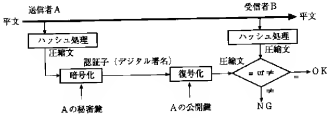
【図２】



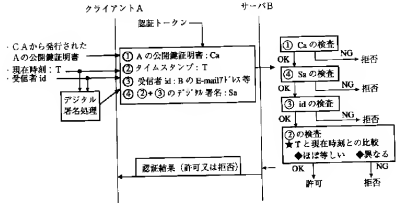
【図３】



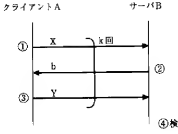
【図４】



【図５】



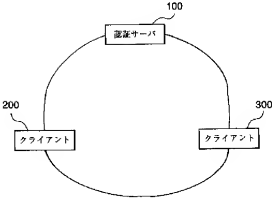
【図９】



【図１４】

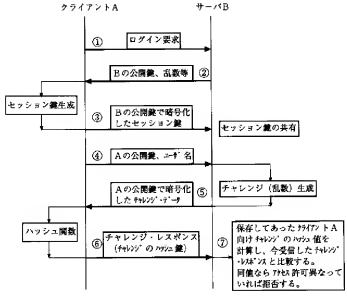
識別名	検査データ	公開鍵
X	Dx = Do	Kpx
W	Dw = Do	Kpy
：	：	：
：	：	：
：	：	：

【図１１】

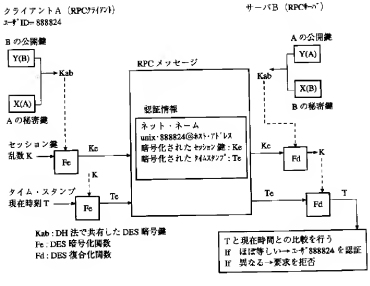


【図１２】

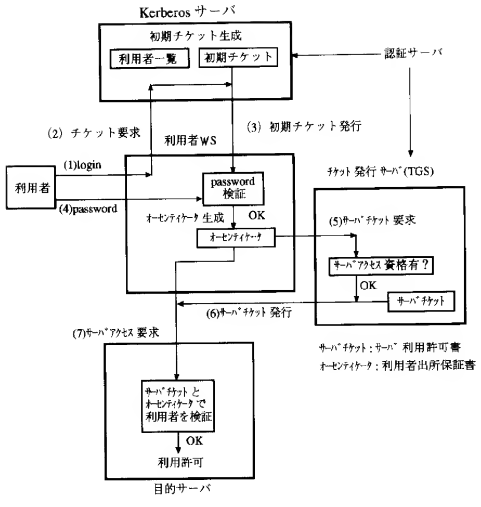
【図６】


クライアントA
サーバB
①
ログイン要求
Bの公開鍵、乱数等
②
セッション鍵生成
③
Bの公開鍵で暗号化したセッション鍵
セッション鍵の共有
④
Aの公開鍵、ユーザ名
Aの公開鍵で暗号化したチャレンジ・データ
⑤
チャレンジ（乱数）生成
ハッシュ関数
⑥
チャレンジ・レスポンス（チャレンジのハッシュ値）
⑦
保存してあったクライアントA向けチャレンジのハッシュ値を計算し、今受信したチャレンジ・レスポンスと比較する。
同値ならアクセス許可異なっていれば拒否する。

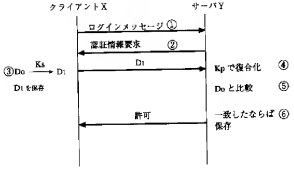
【図７】


クライアントA（RPCクライアント）
ユーザID= 888824
サーバB（RPCサーバ）
Bの公開鍵
Y(B)
Kab
X(A)
Aの秘密鍵
RPCメッセージ
認証情報
ネット・ネーム
unix:888824@ホスト・アドレス
暗号化されたセッション鍵：Ke
暗号化されたタイムスタンプ：Te
Aの公開鍵
Y(A)
Kab
X(B)
Bの秘密鍵
セッション鍵
乱数K
Ke
Fe
K
Kc
Fd
K
タイム・スタンプ
現在時刻T
Te
Fe
Te
Fd
T
Kab：DH法で共有したDES暗号鍵
Fe：DES暗号化関数
Fd：DES復合化関数
Tと現在時間との比較を行う
If　ほぼ等しい→ユーザ888824を認証
If　異なる→要求を拒否

【図８】


Kerberos サーバ
初期チケット生成
利用者一覧
初期チケット
認証サーバ
(2) チケット要求
利用者WS
(3) 初期チケット発行
(1)login
利用者
(4)password
password 検証
オーセンティケータ 生成
OK
オーセンティケータ
チケット発行サーバ(TGS)
(5)サーバチケット要求
サーバアクセス資格有り
OK
サーバチケット
(6)サーバチケット発行
(7)サーバアクセス要求
サーバチケットと オーセンティケータで 利用者を検証
OK
利用許可
目的サーバ
サーバチケット：サーバ利用許可書
オーセンティケータ：利用者出所保証書

【図１５】

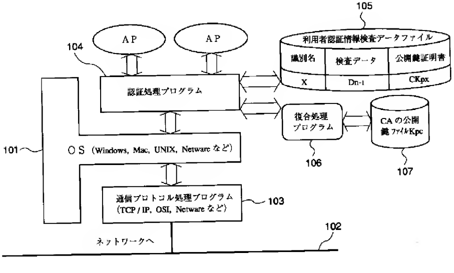

クライアントX
サーバY
ログインメッセージ ①
認証情報要求 ②
D1
③D0 Ka D1
D1を保存
Kpで復合化 ④
D0と比較 ⑤
許可
一致したならば ⑥ 保存

【図１０】

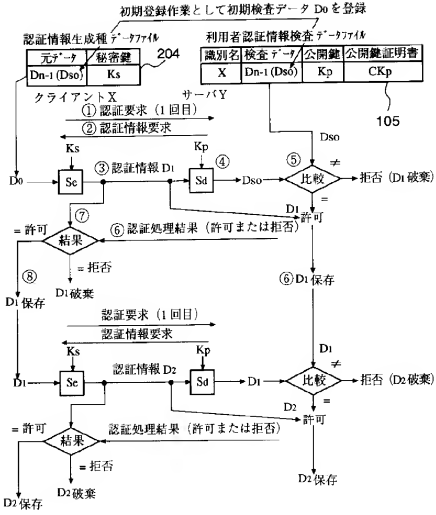
凡例　○：なりすまし可
　　　△：一部なりすまし可
　　　×：なりすまし不可

方式	認証方式＼脅威	「なりすまし」による不正行為者 外部の第三者	「なりすまし」による不正行為者 サーバ管理者	備考
①知識利用	従来のパスワード式	○	○	簡単に盗聴、再利用可能
①知識利用	ワンタイム・パスワード方式	×	△	盗聴内容を再利用できないが、パスワードを使い切ったら再登録処理要
①知識利用	チャレンジ・レスポンス方式	×	○	サーバに侵入されたら辞書攻撃にさらされる
②暗号利用	デジタル署名方式	△	○	盗聴した認証情報の再利用が可能
②暗号利用	デジタル署名付認証トークン方式	△	×	一定時間内であれば盗聴した認証情報の再利用が可能
②暗号利用	SSH(Secure SHell) 方式	△	×	同上
②暗号利用	RPC 認定方式	△	○	同上
②暗号利用	Kerberos 方式	△	○	同上、また集中管理する認証サーバが破られたらそのドメインが全滅する
②暗号利用	ゼロ知識対話証明方式	×	×	対話シーケンスが冗長 認証プロセスが複雑になる
③生体計測	指紋、声紋、手形、網膜パターン、署名、筆記パターン、キーストローク	△	○	オフライン(ローカル)認証では安全性(本人認証精度)が高いがネットワークを介した認証処理の場合は、盗聴による再利用が可能で ① または ② と同様の安全性しかない
④所有物利用	鍵、トークン、バッチ、電子キー、磁気カード、ICカード、非接触型カード	△	○	同上

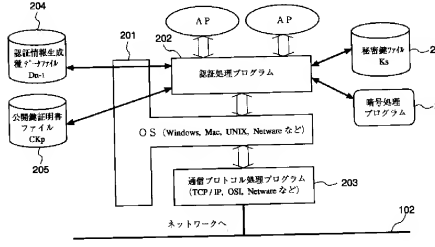
【図１６】



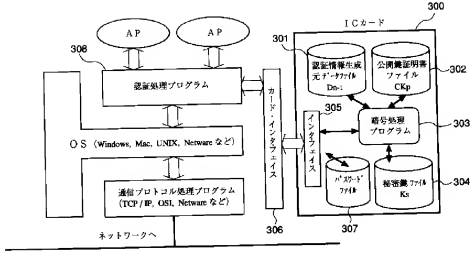
【図１３】


初期登録作業として初期検査データ Do を登録
認証情報生成種データファイル
元データ
秘密鍵
Dn-1 (Dso)
Ks
204
利用者認証情報検査データファイル
識別名
検査データ
公開鍵
公開鍵証明書
X
Dn-1 (Dso)
Kp
CKp
105
クライアントX
サーバY
① 認証要求（1回目）
② 認証情報要求
Dso
Ks
Kp
Do
Se
③ 認証情報 D1
Sd
④
Dso
⑤ 比較
≠
拒否（D1破棄）
=
許可
D1
⑦
= 許可
結果
⑥ 認証処理結果（許可または拒否）
= 拒否
⑧
D1 破棄
⑥ D1 保存
D1 保存
認証要求（1回目）
認証情報要求
Ks
Kp
D1
Se
認証情報 D2
Sd
D1
比較
≠
拒否（D2破棄）
D2
=
許可
= 許可
結果
認証処理結果（許可または拒否）
= 拒否
D2 保存
D2 破棄
D2 保存

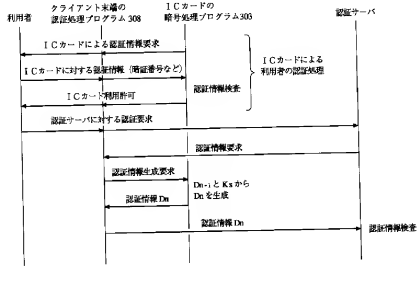
【図１７】


204
認証情報生成種データファイル
Dn-1
201
202
AP
AP
認証処理プログラム
秘密鍵ファイル
Ks
206
暗号処理プログラム
207
公開鍵証明書ファイル
CKp
205
OS（Windows, Mac, UNIX, Netware など）
通信プロトコル処理プログラム
(TCP/IP, OSI, Netware など)
203
ネットワークへ
102

【図１８】



【図１９】



【手続補正書】
【提出日】平成９年９月２５日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　認証要求者からの認証の要求に対して、公開鍵暗号方式により認証者が認証要求者を認証する方法であって、
前もって認証者は、認証要求者の認証情報を検査するための第１の検査情報を保存しておく保存工程と、
前記認証要求者は前記認証者に認証要求を送る認証要求送出工程と、
前記認証者は、前記認証要求者から送られてきた認証要求に対して、認証情報要求を前記認証者に送ることによって応る認証情報要求工程と、
前記認証要求者は、前記認証情報要求に応答して、認証情報を生成するために前記認証要求者が自身が保持している第１の種情報を前記認証要求者の秘密鍵を用いて暗号化して生成した第１の認証情報を前記認証者に送るとともに、生成した前記第１の認証情報を次回の認証要求

のための第２の種情報として前記保持していた第１の種情報に換えて保存する認証情報送出工程と、
前記認証者は、前記認証要求者から送られてきた前記第１の認証情報を前記認証要求者の公開鍵によって復号化することにより、第２の検査情報を生成し、この第２の検査情報を前記前もって保存していた前記第１の検査情報と比較する比較工程と、
前記認証者は、前記第２の検査情報が前記第１の検査情報と一致した場合には、前記認証要求を許可する旨を前記認証要求者に通知すると共に、前記第１の検査情報に代えて前記第１の認証情報を保存する更新工程とを具備することを特徴とする認証方法。
【請求項２】　複数の認証要求者からの認証要求に対して認証を与えるための認証情報を保存する認証サーバであって、
認証要求者毎に認証要求者の認証情報を検査するための検査情報を記憶する手段と、
任意の認証要求者からの認証要求を受けると、認証情報要求メッセージをその認証要求者に送る手段と、
その認証要求者から送られてきた認証情報を、その認証要求者の公開鍵によって復号化して、新たに検査情報を生成し、この新たに生成した検査情報を前記前もって保存していた検査情報と比較する手段と、
前記新たに生成した検査情報が前記保存していた検査情報と一致した場合に、前記認証要求を許可すると共に、前記保存していた検査情報に代えて前記認証要求者から送られてきた認証情報を保存する手段と、を具備する認証サーバ。
【請求項３】　外部の認証サーバの支援により、認証要求者からの認証要求に対する認証を与える認証装置であって、
前記認証要求者を認証する認証情報を生成するための種情報を記憶する記憶手段と、
前記認証サーバに認証要求メッセージを送ると共に、この認証要求メッセージに応答する前記認証サーバからの認証情報要求メッセージを受ける送受信手段と、
前記認証サーバからの認証情報要求メッセージに対して、前記記憶手段に記憶している前記種情報を秘密鍵を用いて暗号化することにより認証情報を生成する暗号化手段と、
生成した認証情報を前記認証サーバに送ると共に、前記記憶手段において、記憶されている前記種情報に換えてこの生成された認証情報を記憶する認証情報送出手段とを具備する認証装置。
【請求項４】　外部の認証サーバの支援により、認証要求者からの記憶媒体を介した認証要求に対して認証を与える認証端末装置であって、
本体と、
認証要求者を認証する認証情報を生成するための種情報とその認証要求者についての秘密鍵と前記種情報から前記秘密鍵を用いて認証情報を生成するプログラムとを記憶する記憶媒体を受け容れるためのインタフェース手段とを有し、
前記本体は、
前記認証要求者からの認証要求を受ける受信手段と、
この認証要求に応答して前記認証サーバに認証要求メッセージを送ると共に、この認証要求に応答する前記認証サーバからの認証情報要求メッセージを受ける要求手段と、
認証情報要求メッセージに応答して、前記インタフェース手段を介して、前記記憶媒体中のプログラムを実行させる指令手段であって、前記プログラムに対して、前記種情報から前記秘密鍵を用いてこの認証要求者の認証情報を生成せしめ、生成した認証情報を前記インタフェース手段を介して前記本体に送り返せしめると共に、この生成した認証情報により前記記憶媒体中の前記種情報を更新せしめる指令手段と、
送り返された認証情報を前記認証サーバに送る認証情報送出手段とを具備する認証端末装置。
【請求項５】　外部の認証サーバの支援により、認証要求者からの認証要求に対する認証を与える認証プログラムを記憶する記憶媒体であって、
前記認証プログラムは、
前記認証要求者を認証する認証情報を生成するための種情報を所定の記憶手段に記憶させる第１のプログラムコードと、
前記認証サーバに認証要求メッセージを送る第２のプログラムコードと、
前記認証サーバからの認証要求メッセージを受け取る第３のプログラムコードと、
認証情報要求メッセージに対して、前記記憶手段に記憶している前記種情報から秘密鍵を用いて認証情報を生成する第４のプログラムコードと、
生成した認証情報を前記認証サーバに送ると共に、前記古い種情報に換えて、この生成した認証情報を新たな種情報として記憶する第５のプログラムコードとを具備することを特徴とする記憶媒体。
【請求項６】　前記認証情報送出工程は、
認証要求を許可する旨の通知を受けた場合に、前記第１の種情報を前記第２の種情報で置き換えて保存し、通知を受けなかった場合には、置き換え保存を行わないことを特徴とする請求項１に記載の認証方法。
【請求項７】　前記認証情報送出手段は、
認証要求を許可する旨の通知を前記認証サーバから受けた場合に、前記種情報の更新を行い、通知を受けなかった場合には、更新を行わないことを特徴とする請求項３に記載の認証装置。
【請求項８】　前記指令手段は、
前記記憶媒体中のプログラムに、認証要求を許可する旨の通知を前記認証サーバから受けた場合に、前記種情報

の更新を行なわせ、通知を受けなかった場合には、更新を行わせないことを特徴とする請求項４に記載の認証端末装置。

【請求項９】　前記第５のプログラムコードは、前記記憶媒体中のプログラムに、認証要求を許可する旨の通知を前記認証サーバから受けた場合に、前記種情報の更新を行ない、通知を受けなかった場合には、更新を行わない第６のプログラムコードを含むことを特徴とする請求項５に記載の記憶媒体。

【請求項１０】　前記第１の種情報の初期値として前記認証要求者の識別情報を用いることを特徴とする請求項１に記載の認証方法。

【請求項１１】　前記種情報の初期値として前記認証要求者の識別情報を用いることを特徴とする請求項３に記載の認証装置。

【請求項１２】　前記種情報の初期値として前記認証要求者の識別情報を用いることを特徴とする請求項４に記載の認証端末装置。

【請求項１３】　前記認証情報送出工程では、認証情報を公開鍵証明書付きで前記認証サーバに送ることを特徴とする請求項１に記載の認証方法。

【請求項１４】　前記認証情報送出手段は、認証情報を公開鍵証明書付きで前記認証サーバに送ることを特徴とする請求項３に記載の認証装置。

【請求項１５】　前記認証情報送出手段は、認証情報を公開鍵証明書付きで前記認証サーバに送ることを特徴とする請求項４に記載の認証端末装置。

【請求項１６】　前記記憶手段は、認証要求者毎の公開鍵を検査情報と共に記憶することを特徴とする請求項２に記載の認証サーバ。

【請求項１７】　認証者は、送られてきた公開鍵証明書を保存することを特徴とする請求項１３に記載の認証方法。

【請求項１８】　前記第１の検査情報が前記第２の検査情報と一致しなかった場合には前記認証要求者による前記認証要求を拒否することを特徴とする請求項１に記載の認証方法。

【請求項１９】　前記新たに生成した検査情報が前記保存していた検査情報と一致しなかった場合には前記認証要求者による前記認証要求を拒否することを特徴とする請求項２に記載の認証サーバ。

【請求項２０】　前記認証要求者の秘密鍵は、真正の持ち主のみが復号化できるように暗号化されていることを特徴とする請求項１に記載の認証方法。

【請求項２１】　前記記憶媒体はＩＣカードであることを特徴とする請求項４に記載の認証端末装置。

【請求項２２】　前記記憶媒体はパスワードを更に記憶し、更に、前記認証要求者から入力されたパスワードと前記記憶媒体に記憶されたパスワードとを比較し、一致したときにのみ、前記記憶媒体は認証情報を前記本体に送り返すことを特徴とする請求項４に記載の認証端末装置。

【請求項２３】　秘密鍵を用いた種情報から認証情報への変換は記憶媒体においてのみ行われ、前記秘密鍵は前記本体側に送られないようにされたことを特徴とする請求項４に記載の認証端末装置。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００４
【補正方法】変更
【補正内容】
【０００４】また、ネットワークセキュリティのための要素技術として、秘匿・保全技術、認証技術、鍵配送技術、否認拒否技術、第三者信用機関、アクセス管理、セキュリティ監査、セキュリティ評価基準などがある。ネットワーク・システムを介した情報通信を行うとき、そのシステムを誰がどのように利用したかということを確認したり、制御、管理することはセキュリティを維持する上において重要であり且つ必須である。システム内で起こる大方のイベントは、情報通信に関わる特定の実体（エンティティ）に起因しているはずであり、従ってそれらの認識はセキュリティ確保の基本であると言える。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正内容】
【００１６】チャレンジ・レスポンス方式は、チャレンジが毎回変化するので、第三者が図中②のメッセージを盗聴していても再利用が不可能であるとの長所がある反面、Ｂ上にＡのパスワードが保持されているので、Ｂの管理者自身がそれを悪用し、クライアントＡになりすまして不正を行うことができるという短所を指摘されている。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００４２
【補正方法】変更
【補正内容】
【００４２】④Ｂは、
Ｘ＝　Ｙ^{2} ｍｏｄ　ｎ　　ｂ＝０の場合
ＺＸ＝Ｙ^{2} ｍｏｄ　ｎ　　ｂ＝１の場合
が成立するかを検査し、これらが成り立てば検査ＯＫとする。ここで、③及び④でｂ＝０およびｂ＝１の場合に分けているのは、Ａになりすました悪意のクライアントＡ′はＴの値を知らなくても次のようにして検査に合格できるからである。即ち、常にｂ＝１であるなら、Ａは①でＹの値として適当なＹ′を定め、Ｘ＝（Ｙ′）^{2}／Ｚ ｍｏｄ　ｎを計算し、このＸをＢに送る。次に③でＹ＝Ｙ′の値を送ると④の検査は当然合格する。また、この

方式では、ｂの値を予想してから検査式を満たすＸとＹを計算できるので繰り返し１回当たりのなりすまし確率は１／２である。従ってこの手順をｋ回繰り返すとなりすまし確率を2^{-k}にできる。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００５４
【補正方法】変更
【補正内容】
【００５４】例えば、ワンタイム・パスワード方式（S/Key等）はこの要件を満たしているが、デジタル署名付認証トークン方式はそのタイムスタンプの許容時間内であれば盗聴トークンが再利用出来てしまう。
（２）認証サーバに認証情報が保存されないこと。換言すれば、認証サーバは利用者個々の認証情報を保管する必要がなく、ただログイン時の認証情報が正当か否かを識別できる機能を有すればよい。これによって、たとえ悪意の第三者が認証サーバに侵入できたとしても利用者個々の認証情報を得ることは出来ない。
（３）認証シーケンスは極力簡単であること。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００５７
【補正方法】変更
【補正内容】
【００５７】
【課題を解決するための手段】上記課題を達成するための本発明の、認証要求者からの認証の要求に対して、公開鍵暗号方式により認証者が認証要求者を認証する方法は、前もって認証者は、認証要求者の認証情報を検査するための第１の検査情報を保存しておく保存工程と、前記認証要求者は前記認証者に認証要求を送る認証要求送出工程と、前記認証者は、前記認証要求者から送られてきた認証要求に対して、認証情報要求を前記認証者に送ることによって応る認証情報要求工程と、前記認証要求者は、前記認証情報要求に応答して、認証情報を生成するために前記認証要求者が自身が保持している第１の種情報を前記認証要求者の秘密鍵を用いて暗号化して生成した第１の認証情報を前記認証者に送るとともに、生成した前記第１の認証情報を次回の認証要求のための第２の種情報として前記保持していた第１の種情報に換えて保存する認証情報送出工程と、前記認証者は、前記認証要求者から送られてきた前記第１の認証情報を前記認証要求者の公開鍵によって復号化することにより、第２の検査情報を生成し、この第２の検査情報を前記前もって保存していた前記第１の検査情報と比較する比較工程と、前記認証者は、前記第２の検査情報が前記第１の検査情報と一致した場合には、前記認証要求を許可する旨を前記認証要求者に通知するとともに、前記第１の検査情報に代えて前記第１の認証情報を保存する更新工程とを具備することを特徴とする。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００６０
【補正方法】変更
【補正内容】
【００６０】この認証方法を適用するために、本発明にかかる、複数の認証要求者からの認証要求に対して認証を与えるための認証情報を保存する認証情報ファイルサーバは、認証要求者毎に認証要求者の認証情報を検査するための検査情報を記憶する手段と、任意の認証要求者からの認証要求を受けると、認証情報要求メッセージをその認証者に送る手段と、その認証要求者から送られてきた認証情報を、その認証要求者の公開鍵によって復号化して、新たに検査情報を生成し、この新たに生成した検査情報を前記前もって保存していた検査情報と比較する手段と、前記新たに生成した検査情報が前記保存していた検査情報と一致した場合に、前記認証要求を許可すると共に、前記保存していた検査情報に代えて前記認証要求者から送られてきた認証情報を保存する手段とを具備する。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００７８
【補正方法】変更
【補正内容】
【００７８】第１３図の例では、クライアントＸの初期種データはD_{S0}として登録されている。本実施形態の認証プロトコルは、クライアントＸは、始めての認証セッションでは、認証情報をこの初期種データD_{S0}から生成する。認証が許可された場合には、今まで保存していた種データD_{n-1}をクライアントＸの秘密鍵K_Sで暗号化し、それを次回の認証セッションのための種データD_nとして保存する点に大きな特徴がある。尚、前回の種データD_{n-1}は次回以降のログインでは使用されることはないが、履歴の保持のために保存しておいても良い。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００８４
【補正方法】変更
【補正内容】
【００８４】・ステップ⑦
サーバからの認証処理結果を受けたクライアントでは、その認証処理結果が許可かまたは拒否であるかを判断する。
・ステップ⑧
認証が許可されたものであった場合には、サーバ側に送っていた認証情報D_1を次回のログイン時の種データD_1としてファイル２０４に記憶する。
【手続補正１０】

【補正対象書類名】明細書
【補正対象項目名】００９８
【補正方法】変更
【補正内容】
【００９８】サーバ側の認証処理プログラム１０４は、クライアントXのログインメッセージを受信すると、クライアントに認証情報要求メッセージを返し、このメッセージに対してクライアントXから送信される認証情報を受信すると、認証情報と共に送信されてきた利用者Xの公開鍵証明書に付されている証明局ＣＡのディジタル署名を、証明局ＣＡの公開鍵K_{pc}（ファイル１０７中に保存されている）を用いて検査する。検査が確認されたならば、その公開鍵証明書はクライアントXの正当な公開鍵証明書であることが確認される。また、クライアントXの公開鍵証明書CK_{px}をファイル１０５に保存する。プログラム１０６は、データファイル１０５にアクセスして、公開鍵証明書CK_{px}中のクライアントXの公開鍵K_{px}を取り出す。
【手続補正１２】
【補正対象書類名】図面
【補正対象項目名】図１３
【補正方法】変更
【補正内容】
【図１３】